CIPHERING METHOD, DECIPHERING METHOD, CIPHERING DEVICE, DECIPHERING DEVICE AND RECORDING MEDIUM

Patent Number: JP2000115551
Publication date: 2000-04-21
Inventor(s): YOKOUCHI KOJI
Applicant(s): FUJI PHOTO FILM CO LTD
Requested Patent: JP2000115551
Application Number: JP19980278772 19980930
Priority Number(s):
IPC Classification: H04N1/44; G09C1/00; H04L9/06; H04N7/167
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To reduce the processing time for ciphering compared with the case of ciphering all of image data.
SOLUTION: Plural image data is inputted and stored (step 200) and a difference of each image element between one of the plural image data (first image data) and image data excepting for first image data is calculated to be stored as difference data (steps 202 and 204). First image data is ciphered to be stored as ciphered data (step 206) and ciphered data and difference data are retained in a floppy disk as ciphered image data (step 208).

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－115551
(P2000－115551A)
(43)公開日　平成12年４月21日(2000.4.21)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
H04N 1/44		H04N 1/44		5C064
G09C 1/00	610	G09C 1/00	610A	5C075
H04L 9/06		H04L 9/00	611Z	5J104
H04N 7/167		H04N 7/167		

審査請求　未請求　請求項の数10　ＯＬ　（全 12 頁）

(21)出願番号　特願平10－278772

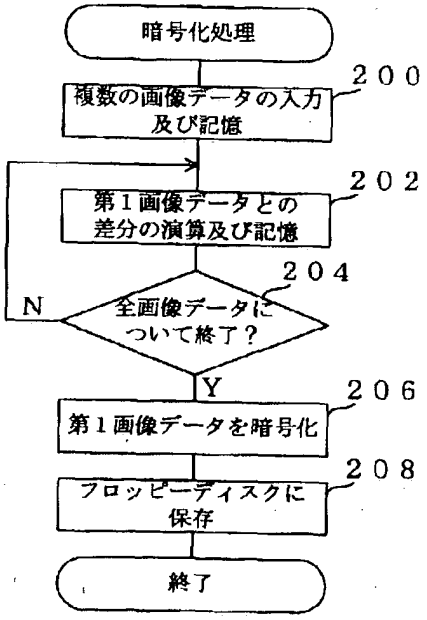
(22)出願日　平成10年９月30日(1998.9.30)

(71)出願人　000005201
富士写真フイルム株式会社
神奈川県南足柄市中沼210番地
(72)発明者　横内　康治
神奈川県足柄上郡開成町宮台798番地　富士写真フイルム株式会社内
(74)代理人　100079049
弁理士　中島　淳　（外３名）

Ｆターム(参考)　5C064 CA14 CC04 CC06
5C075 EE03 FF03 FF90
5J104 AA18 CA02 NA02 NA27 PA14

(54)【発明の名称】　暗号化方法、復号化方法、暗号化装置、復号化装置及び記録媒体

(57)【要約】
【課題】　処理時間を短縮することができる暗号化方法、復号化方法、暗号化装置、復号化装置及び記録媒体を得る。
【解決手段】　複数の画像データを入力して記憶し（ステップ２００）、該複数の画像データのうちの１つ（第１画像データ）と該第１画像データ以外の画像データとの画素毎の差分を算出して差分データとして記憶し（ステップ２０２、２０４）、上記第１画像データを暗号化して暗号化データとして記憶し（ステップ２０６）、上記暗号化データ及び差分データを暗号化画像データとしてフロッピーディスクに保存する（ステップ２０８）。



1

【特許請求の範囲】

【請求項１】　各々画像を表す複数の画像データのうちの一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データを求め、前記複数の画像データのうちの残りの画像データについては前記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りの画像データに対応する差分データを求めることによって前記複数の画像データに対応する暗号化画像データを生成する暗号化方法。

【請求項２】　請求項１記載の暗号化方法によって生成された暗号化画像データを復号化する復号化方法であって、

前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、

前記差分データについては差分データを求める際に前記暗号化する画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化する画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求めることによって前記暗号化画像データに対応する復号化画像データを生成する復号化方法。

【請求項３】　１画像を表す画像データを複数のブロックに分割し、

一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データを求め、前記複数のブロックの画像データのうちの残りのブロックの画像データについては前記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りのブロックの画像データに対応する差分データを求めることによって前記１画像を表す画像データに対応する暗号化画像データを生成する暗号化方法。

【請求項４】　請求項３記載の暗号化方法によって生成された暗号化画像データを復号化する復号化方法であって、

前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、

前記差分データについては差分データを求める際に前記暗号化するブロックの画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化するブロックの画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求めることによって前記暗号化画像データに対応する復号化画像データを生成する復号化方法。

2

【請求項５】　各々画像を表す複数の画像データを入力する画像データ入力手段と、

入力された一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データを求め、入力された残りの画像データについては前記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りの画像データに対応する差分データを求める暗号化手段と、

前記暗号化データと前記差分データとを前記複数の画像データに対応する暗号化画像データとして出力する暗号データ出力手段と、

を備えた暗号化装置。

【請求項６】　請求項５記載の暗号化装置によって生成された暗号化画像データを復号化する復号化装置であって、

前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化する画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化する画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求める復号化手段を備えた復号化装置。

【請求項７】　１画像を表す画像データを入力する画像データ入力手段と、

入力された画像データを複数のブロックに分割するブロック化手段と、

一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データを求め、前記複数のブロックの画像データのうちの残りのブロックの画像データについては前記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りのブロックの画像データに対応する差分データを求める暗号化手段と、

前記暗号化データと前記差分データとを前記１画像を表す画像データに対応する暗号化画像データとして出力する画像データ出力手段と、

を備えた暗号化装置。

【請求項８】　請求項７記載の暗号化装置によって生成された暗号化画像データを復号化する復号化装置であって、

前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化するブロックの画

像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化するブロックの画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求める復号化手段を備えた復号化装置。

【請求項９】　請求項１乃至請求項４記載のいずれかの発明における処理をコンピュータに実行させるためのプログラムを記録した記録媒体。

【請求項１０】　請求項１又は請求項３記載の発明における処理によって生成された暗号化画像データを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号化方法、復号化方法、暗号化装置、復号化装置及び記録媒体に係り、特に、デジタル化された画像データを暗号化する暗号化方法、該暗号化方法を適用可能な暗号化装置、前記暗号化方法をコンピュータで実行させるためのプログラムを記録した記録媒体、前記暗号化方法によって得られた暗号化画像データを記録した記録媒体、前記暗号化方法によって得られた暗号化画像データを復号化する復号化方法、該復号化方法を適用可能な復号化装置、前記復号化方法をコンピュータで実行させるためのプログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】従来の画像データに対する暗号化の技術としては、例えば、特開平６－１２５５５３号公報に記載の技術があった。

【０００３】この特開平６－１２５５５３号公報に記載の技術では、暗号化のための処理量を低減することを目的として、画像データに対してＤＣＴ変換（離散コサイン変換）を行なうことによって得られた信号のうちの直流成分のみを暗号化していた。

【０００４】

【発明が解決しようとする課題】しかしながら、上記特開平６－１２５５５３号公報に記載されている技術等の従来の暗号化技術では、暗号化強度を強くするほど、暗号化及び該暗号化によって得られた暗号化画像データの復号化の双方の処理量が多くなるので、暗号化及び復号化のための処理時間が長くなる、という問題点があった。

【０００５】また、各々１枚の画像を示す複数の画像データの各々について暗号化及び復号化を行なう場合には、画像データの数に比例して暗号化及び復号化のための処理時間が増加することはいうまでもない。

【０００６】本発明は上記問題点を解消するために成されたものであり、処理時間を短縮することができる暗号化方法、復号化方法、暗号化装置、復号化装置及び記録媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】上記目的を達成するために、請求項１記載の暗号化方法は、各々画像を表す複数の画像データのうちの一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データを求め、前記複数の画像データのうちの残りの画像データについては前記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りの画像データに対応する差分データを求めることによって前記複数の画像データに対応する暗号化画像データを生成する。

【０００８】また、請求項５記載の暗号化装置は、各々画像を表す複数の画像データを入力する画像データ入力手段と、入力された一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データを求め、入力された残りの画像データについては前記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りの画像データに対応する差分データを求める暗号化手段と、前記暗号化データと前記差分データとを前記複数の画像データに対応する暗号化画像データとして出力する暗号データ出力手段と、を備えている。

【０００９】請求項１に記載の暗号化方法及び請求項５に記載の暗号化装置によれば、各々画像を表す複数の画像データのうちの一部の画像データについては暗号化することにより該一部の画像データに対応する暗号化データが求められ、上記複数の画像データのうちの残りの画像データについては上記暗号化する画像データと直接的又は間接的に画素毎の差分を演算することにより上記残りの画像データに対応する差分データが求められ、これによって上記複数の画像データに対応する暗号化画像データが生成される。

【００１０】ここで、上記暗号化する画像データと間接的に画素毎の差分を演算する場合には、例えば、暗号化データを求める画像データを第１画像データとし、差分データを求める画像データを第Ｎ画像データ（Ｎ＝２，３，・・・）とした場合、第Ｎ画像データの差分データを求める際の対象を第（Ｎ－１）画像データとする場合等が含まれる。但し、この場合、第２画像データの差分データを第１画像データとの差分の演算によって求めることのみは、上記の「直接的」に相当する。

【００１１】このように、請求項１に記載の暗号化方法及び請求項５に記載の暗号化装置によれば、複数の画像データの全てを暗号化せずに、一部の画像データのみを暗号化し、残りの画像データについては暗号化する画像データと直接的又は間接的に画素毎の差分を演算することによって全ての暗号化画像データを生成しているの

で、全ての画像データに対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができる。

【００１２】また、請求項２記載の復号化方法は、請求項１記載の暗号化方法によって生成された暗号化画像データを復号化する復号化方法であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化する画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化する画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求めることによって前記暗号化画像データに対応する復号化画像データを生成する。

【００１３】また、請求項６記載の復号化装置は、請求項５記載の暗号化装置によって生成された暗号化画像データを復号化する復号化装置であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化する画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化する画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求める復号化手段を備えている。

【００１４】請求項２に記載の復号化方法及び請求項６に記載の復号化装置は各々、請求項１及び請求項５記載の発明によって生成された暗号化画像データを復号化する復号化方法及び復号化装置であって、上記暗号化データについては復号化して該暗号化データに対応する画像データが求められ、上記差分データについては差分データを求める際に上記暗号化する画像データと直接的に差分を演算した場合は上記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データが求められ、差分データを求める際に上記暗号化する画像データと間接的に差分を演算した場合は上記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データが求められ、これによって上記暗号化画像データに対応する復号化画像データが生成される。

【００１５】このように、請求項２に記載の復号化方法及び請求項６に記載の復号化装置によれば、暗号化画像データの全てを復号化せずに、実際に暗号化された暗号化データのみを復号化し、残りの画像データについては復号化した画像データ又は復号化した画像データに基づく画像データとの加算を行なうことによって全ての復号化画像データを生成しているので、全ての画像データに対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる。

【００１６】また、請求項３記載の暗号化方法は、１画像を表す画像データを複数のブロックに分割し、一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データを求め、前記複数のブロックの画像データのうちの残りのブロックの画像データについては前記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りのブロックの画像データに対応する差分データを求めることによって前記１画像を表す画像データに対応する暗号化画像データを生成する。

【００１７】また、請求項７記載の暗号化装置は、１画像を表す画像データを入力する画像データ入力手段と、入力された画像データを複数のブロックに分割するブロック化手段と、一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データを求め、前記複数のブロックの画像データのうちの残りのブロックの画像データについては前記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより前記残りのブロックの画像データに対応する差分データを求める暗号化手段と、前記暗号化データと前記差分データとを前記１画像を表す画像データに対応する暗号化画像データとして出力する画像データ出力手段と、を備えている。

【００１８】請求項３に記載の暗号化方法及び請求項７に記載の暗号化装置によれば、１画像を表す画像データが複数のブロックに分割され、一部のブロックの画像データについては暗号化することにより該一部のブロックの画像データに対応する暗号化データが求められ、上記複数のブロックの画像データのうちの残りのブロックの画像データについては上記暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することにより上記残りのブロックの画像データに対応する差分データが求められ、これによって上記１画像を表す画像データに対応する暗号化画像データが生成される。

【００１９】ここで、上記暗号化するブロックの画像データと間接的に画素毎の差分を演算する場合には、例えば、暗号化データを求めるブロックの画像データを第１画像データとし、差分データを求めるブロックの画像データを第Ｎブロックの画像データ（Ｎ＝２，３，・・・）とした場合、第Ｎブロックの画像データの差分データを求める際の対象を第（Ｎ－１）ブロックの画像データとする場合等が含まれる。但し、この場合、第２ブロ

ックの画像データの差分データを第１ブロックの画像データとの差分の演算によって求めることのみは、上記の「直接的」に相当する。

【００２０】このように、請求項３に記載の暗号化方法及び請求項７に記載の暗号化装置によれば、１画像を表す画像データの全ての領域を暗号化せずに、一部のブロックの画像データのみを暗号化し、残りのブロックの画像データについては暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することによって全体的な暗号化画像データを生成しているので、画像データの全ての領域に対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができる。

【００２１】また、請求項４記載の復号化方法は、請求項３記載の暗号化方法によって生成された暗号化画像データを復号化する復号化方法であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化するブロックの画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化するブロックの画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求めることによって前記暗号化画像データに対応する復号化画像データを生成する。

【００２２】また、請求項８記載の復号化装置は、請求項７記載の暗号化装置によって生成された暗号化画像データを復号化する復号化装置であって、前記暗号化データについては復号化して該暗号化データに対応する画像データを求め、前記差分データについては差分データを求める際に前記暗号化するブロックの画像データと直接的に差分を演算した場合は前記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に前記暗号化するブロックの画像データと間接的に差分を演算した場合は前記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求める復号化手段を備えている。

【００２３】請求項４に記載の復号化方法及び請求項８に記載の復号化装置は各々、請求項３及び請求項７記載の発明によって生成された暗号化画像データを復号化する復号化方法及び復号化装置であって、上記暗号化データについては復号化して該暗号化データに対応する画像データが求められ、上記差分データについては差分データを求める際に上記暗号化するブロックの画像データと直接的に差分を演算した場合は上記暗号化データに対応する画像データに差分データを画素毎に加算することにより差分データに対応する画像データを求め、差分データを求める際に上記暗号化するブロックの画像データと間接的に差分を演算した場合は上記暗号化データに対応する画像データに基づいて求めた画像データに差分データを画素毎に加算することにより差分データに対応する画像データが求められ、これによって上記暗号化画像データに対応する復号化画像データが生成される。

【００２４】このように、請求項４に記載の復号化方法及び請求項８に記載の復号化装置によれば、暗号化画像データの全ての領域を復号化せずに、一部の領域の画像データに対応する暗号化データのみを復号化し、残りの領域の画像データについては復号化した画像データ又は復号化した画像データに基づいて求めた画像データとの加算を行なうことによって全ての領域の復号化画像データを生成しているので、画像データの全ての領域に対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる。

【００２５】また、請求項９記載の記録媒体は、請求項１乃至請求項４記載のいずれかの発明における処理をコンピュータに実行させるためのプログラムが記録されている。

【００２６】従って、コンピュータが前記記録媒体に記録されているプログラムを読み出して実行することにより、請求項１乃至請求項４記載の発明と同様の効果を奏することができる。

【００２７】更に、請求項１０記載の記録媒体は、請求項１又は請求項３記載の発明における処理によって生成された暗号化画像データが記録されている。

【００２８】従って、この記録媒体に記録された暗号化画像データを請求項２及び請求項４記載の発明によって復号化する場合、復号化に要する処理時間は非常に短い。

【００２９】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態について詳細に説明する。

【００３０】〔第１実施形態〕図１に示すように、本第１実施形態に係る暗号化装置及び復号化装置としての暗号化復号化装置１０は、パーソナルコンピュータ又はワークステーション等で構成されている。即ち、ディスプレイ３２、ワークステーション１２、及びワークステーション１２に接続された各種の入出力機器を備えている。

【００３１】ワークステーション１２は、図２に示すように、ＣＰＵ１４、ＲＯＭ１６、ＲＡＭ１８及び入出力ポート２０を備え、これらはバスによって互いに接続されている。

【００３２】更に、入出力ポート２０にはフロッピーディスクに記録された原画像データ、暗号化画像データ等の読み取りやフロッピーディスクへの暗号化画像デー

タ、復号化画像データ（原画像データ）等の書き込み等に用いられるフロッピーディスクドライブ２６が接続されていると共に、暗号化復号化装置１０を暗号化装置及び復号化装置として作用させるための暗号化処理プログラム及び復号化処理プログラム等が記憶された記憶装置２２が接続されている。暗号化処理プログラム及び復号化処理プログラムは、オペレータからの指示に応じて選択的に読み出されて実行される。

【００３３】本第１実施形態では入出力ポート２０に接続される入出力機器として、フロッピーディスクドライブ２６及び記憶装置２２以外に、オペレータが暗号化処理及び復号化処理の何れの処理を行なうのかの指示等を入力するためのキーボード２４及びマウス２８が用いられている。

【００３４】次に、図３を参照して、暗号化復号化装置１０を暗号化装置として動作させた場合の暗号化復号化装置１０の作用について説明する。なお、図３は、オペレータによって暗号化処理の指示が入力された際に記憶装置２２から読み出されて実行される暗号化処理プログラムの概略フローチャートである。

【００３５】まずステップ２００では、フロッピーディスクドライブ２６にセットされているフロッピーディスクに記録されている各々１枚の画像を表す複数の画像データを入力して記憶装置２２の所定領域に記憶する。

【００３６】次のステップ２０２では、上記ステップ２００において入力及び記憶された複数の画像データのうちの１つの画像データ（以下、第１画像データという。）と該第１画像データ以外の何れかの画像データとの画素毎の差分（以下、差分データという。）を算出して記憶装置２２の対応する画像データの記憶領域に記憶（上書き）する。

【００３７】次のステップ２０４では、第１画像データ以外の全ての画像データについて第１画像データとの差分の算出及び記憶が終了したか否かを判定し、終了していない場合は上記ステップ２０２へ戻り、終了した時点でステップ２０６に移行する。

【００３８】次のステップ２０６では、上記第１画像データに対して暗号化を行ない、記憶装置２２に記憶する。この暗号化の方法としては、公開鍵方式、共通鍵方式等のあらゆる既存の暗号化技術を適用することができる。

【００３９】次のステップ２０８では、上記ステップ２０６によって記憶装置２２に記憶された第１画像データの暗号化データと上記ステップ２０２及び２０４の繰り返し処理によって記憶装置２２に記憶された第１画像データ以外の画像データの差分データとをフロッピーディスクドライブ２６によってフロッピーディスクの空き領域に出力した後、本暗号化処理プログラムを終了する。

【００４０】図４には、複数の画像（コマ画像）が記録された1 本の写真フィルムの各画像に対応する複数の画像データを図３に示した暗号化処理プログラムの処理対象とした場合の暗号化画像データ生成の流れが示されている。

【００４１】同図に示すように、図３のステップ２００の処理によってフロッピーディスクから入力された写真フィルム１本分の複数のコマ画像に各々対応する第１画像データ１０１、第２画像データ１０２、第３画像データ１０３、・・・のうちの第１画像データ１０１（ステップ２０６において暗号化される画像データ）以外の画像データは、ステップ２０２及び２０４の繰り返し処理によって、第１画像データとの画素毎の差分が算出され、算出された差分データが差分データ１０２’、差分データ１０３’、・・・として記憶される。

【００４２】その後、ステップ２０６の処理によって第１画像データ１０１が暗号化されて暗号化データ１０１’として記憶される。

【００４３】最後にステップ２０８の処理によって、以上の結果得られた暗号化データ１０１’、差分データ１０２’、差分データ１０３’、・・・が写真フィルム１本分の暗号化画像データとしてフロッピーディスクに保存される。

【００４４】次に、図５を参照して、暗号化復号化装置１０を復号化装置として動作させた場合の暗号化復号化装置１０の作用について説明する。なお、図５は、オペレータによって復号化処理の指示が入力された際に記憶装置２２から読み出されて実行される復号化処理プログラムの概略フローチャートである。

【００４５】まずステップ２５０では、フロッピーディスクに記録されている復号化の対象とする暗号化画像データをフロッピーディスクドライブ２６によって入力して記憶装置２２の所定領域に記憶する。

【００４６】次のステップ２５２では、上記第１画像データに相当する暗号化データに対して復号化を行ない、この結果得られた画像データ、すなわち第１画像データを記憶装置２２に記憶する。ここでの復号化方法は暗号化方法に対応した方法とされる。

【００４７】次のステップ２５４では、上記ステップ２５２によって記憶された第１画像データと、上記ステップ２５０によって入力及び記憶された暗号化画像データのうちの上記第１画像データ以外の画像データに対応する差分データの１つとの画素毎の和分を算出して記憶装置２２の対応する差分データの記憶領域に記憶（上書き）する。本ステップ２５４によって算出された値は、算出に用いた差分データに対応する画像データに相当する。

【００４８】次のステップ２５６では、全ての差分データについて上記第１画像データとの和分の算出及び記憶が終了したか否かを判定し、終了していない場合は上記ステップ２５４へ戻り、終了した時点でステップ２５８に移行する。

【００４９】次のステップ２５８では、上記ステップ２５２によって記憶装置２２に記憶された第１画像データと上記ステップ２５４及び２５６の繰り返し処理によって記憶装置２２に記憶された第１画像データ以外の画像データとをフロッピーディスクドライブ２６によってフロッピーディスクの空き領域に出力した後、本復号化処理プログラムを終了する。

【００５０】図６には、複数の画像（コマ画像）が記録された1 本の写真フィルムの各画像に対応する複数の画像データを図３に示した暗号化処理プログラムで暗号化することによって得られた暗号化画像データを図５に示した復号化処理プログラムの処理対象とした場合の復号化画像データ（原画像データ）生成の流れが示されている。

【００５１】同図に示すように、図５のステップ２５０の処理によってフロッピーディスクから入力された写真フィルム１本分の複数のコマ画像に各々対応する暗号化データ１０１’、差分データ１０２’、差分データ１０３’、・・・のうちの暗号化データ１０１’は、ステップ２５２の処理によって復号化されて第１画像データ１０１として記憶される。

【００５２】その後、ステップ２５４及び２５６の繰り返し処理によって、第１画像データ１０１と差分データ１０２’、１０３’、・・・との画素毎の和分が算出され、算出された和分が第２画像データ１０２、第３画像データ１０３、・・・として記憶される。

【００５３】最後にステップ２５８の処理によって、以上の結果得られた第１画像データ１０１、第２画像データ１０２、第３画像データ１０３、・・・が写真フィルム１本分の復号化画像データ（原画像データ）としてフロッピーディスクに保存される。

【００５４】以上詳細に説明したように、本第１実施形態に係る暗号化復号化装置では、暗号化を行なう場合には、暗号化の対象とする複数の画像の画像データの全てを暗号化せずに、1 枚の画像に対応する画像データのみを暗号化し、他の画像データについては暗号化する画像データとの差分のみを演算することによって全ての暗号化画像データを生成しているので、全ての画像データに対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができると共に、復号化を行なう場合には、暗号化画像データの全てを復号化せずに、1 枚の画像に対応する暗号化データのみを復号化し、他の画像データについては復号化した画像データとの和分のみを演算することによって全ての復号化画像データを生成しているので、全ての画像データに対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる。

【００５５】なお、本第１実施形態では、第１画像データ以外の画像データの差分を算出する際の対象を第１画像データとした場合について説明したが、本発明はこれに限定されるものではなく、例えば、第１画像データ以外の第Ｎ画像データ（Ｎ＝２、３、・・・）の差分を算出する際の対象を第（Ｎ－１）画像データとすることもできる。このように暗号化画像データを生成した場合、該暗号化画像データを復号する際には暗号化された第１画像データを暗号化方法に対応した復号化方法によって復号した後に、この復号された第１画像データに第２画像データに対応する差分データを画素毎に加算することによって第２画像データを復元し、この第２画像データに対して第３画像データに対応する差分データを画素毎に加算することによって第３画像データを復元する、という手順を第１画像データ以外の全ての画像データについて繰り返すことによって全ての画像データを再現することができる。

【００５６】また、本第１実施形態では、実際に暗号化を行なう画像データを１つの画像データのみとした場合について説明したが、本発明はこれに限定されるものではなく、複数の画像データについて暗号化する形態としてもよい。

【００５７】また、本第１実施形態では、暗号化処理の途中段階で生成される暗号化データ１０１’、差分データ１０２’、・・・や復号化処理の途中段階で生成される第１画像データ１０１、第２画像データ１０２、・・・を記憶装置２２に記憶する場合について説明したが、本発明はこれに限定されるものではなく、フロッピーディスクに直接記録する形態としてもよい。

【００５８】また、本第１実施形態では、差分データを算出する場合の領域を当該画像データの全ての領域とした場合について説明したが、本発明はこれに限定されるものではなく、当該画像データの一部の領域とする形態としてもよい。従って、例えば、第１画像データ１０１及び第２画像データ１０２の各々のサイズが異なる場合でも差分データを算出することが可能である。

【００５９】また、本第１実施形態では、差分データの各々が、どの画像データとの差分であるのか、といった情報を暗号化画像データに保持しない場合について説明したが、本発明はこれに限定されるものではなく、この情報を保持する形態としてもよい。

【００６０】また、本第１実施形態では、暗号化処理プログラム及び復号化処理プログラムを記憶装置２２に記録しているが、本発明はこれに限定されるものではなく、該プログラムをフロッピーディスクに記憶すると共に、ワークステーション１２にハードディスクを備え、フロッピーディスクから該プログラムを読み取り、ハードディスクにインストールしてもよい。また、有線又は無線のネットワークに電話回線等の伝送手段により伝送してインストールしてもよい。なお、該プログラムをフロッピーディスクに記憶することに限定されず、ＣＤ－ＲＯＭ、磁気テープに該プログラムを格納し、該ＣＤ－ＲＯＭ、磁気テープからパソコンのハードディスクにイ

ンストールしてもよい。また、該プログラムを格納したハードディスクを備えるようにしてもよい。更に、パソコンのハードディスクやＲＡＭに直接プログラムを書き込むようにしてもよい。このように上記プログラムは、有形の記憶媒体及び伝送手段の少なくとも一方により流通することができる。

【００６１】また、本第１実施形態では、暗号化画像データをフロッピーディスクに記録する場合について説明したが、本発明はこれに限定されるものではなく、ハードディスク等の磁気ディスク、ＣＤ－Ｒ等の光ディスク、光磁気ディスク等に記録する形態としてもよい。この場合、上記ハードディスク、ＣＤ－Ｒ等の各メディアが本発明の請求項１０記載の記録媒体に相当することになる。

【００６２】〔第２実施形態〕次に、本発明の第２実施形態について説明する。なお、本第２実施形態に係る暗号化装置及び復号化装置としての暗号化復号化装置の構成は、上記第１実施形態（図１及び図２参照）と同様であるので、ここでの説明は省略する。

【００６３】まず、図７を参照して、本第２実施形態に係る暗号化復号化装置１０を暗号化装置として動作させた場合の暗号化復号化装置１０の作用について説明する。なお、図７は、オペレータによって暗号化処理の指示が入力された際に記憶装置２２から読み出されて実行される暗号化処理プログラムの概略フローチャートである。

【００６４】まずステップ３００では、フロッピーディスクドライブ２６にセットされているフロッピーディスクに記録されている暗号化の対象とする画像データを入力して記憶装置２２の所定領域に記憶する。

【００６５】次のステップ３０２では、上記ステップ３００において入力及び記憶された画像データを所定の大きさのブロックに分割する。

【００６６】次のステップ３０４では、上記ステップ３０２において分割された画像データのうちの１つのブロック（以下、第１ブロックという。）の画像データと該第１ブロック以外のブロックの何れかのブロックの画像データとの画素毎の差分（以下、差分データという。）を算出して記憶装置２２の対応するブロックの記憶領域に記憶（上書き）する。

【００６７】次のステップ３０６では、第１ブロック以外の全てのブロックの画像データについて上記第１ブロックの画像データとの画素毎の差分の算出及び記憶が終了したか否かを判定し、終了していない場合は上記ステップ３０４へ戻り、終了した時点でステップ３０８に移行する。

【００６８】次のステップ３０８では、上記第１ブロックの画像データに対して暗号化を行ない、記憶装置２２に記憶する。この暗号化の方法としては、公開鍵方式、共通鍵方式等のあらゆる既存の暗号化技術を適用することができる。

【００６９】次のステップ３１０では、上記ステップ３０８によって記憶装置２２に記憶された第１ブロックの画像データの暗号化データと上記ステップ３０４及び３０６の繰り返し処理によって記憶装置２２に記憶された第１ブロック以外のブロックの画像データの差分データとをフロッピーディスクドライブ２６によってフロッピーディスクの空き領域に出力した後、本暗号化処理プログラムを終了する。

【００７０】図８には、１枚の長尺状の画像に対応する画像データを図７に示した暗号化処理プログラムの処理対象とした場合の暗号化画像データ生成の流れが示されている。

【００７１】同図に示すように、図７のステップ３００の処理によってフロッピーディスクから入力された画像データ１２０は、ステップ３０２の処理によって第１ブロック１２１、第２ブロック１２２、第３ブロック１２３、・・・に分割される。

【００７２】その後、第１ブロック１２１、第２ブロック１２２、第３ブロック１２３、・・・のうちの第１ブロック１２１（ステップ３０８において暗号化されるブロック）以外のブロックの画像データについては、ステップ３０４及び３０６の繰り返し処理によって、第１ブロック１２１の画像データとの画素毎の差分が算出され、算出された差分が差分データ１２２’、差分データ１２３’、・・・として記憶される。

【００７３】その後、ステップ３０８の処理によって第１ブロック１２１の画像データが暗号化されて暗号化データ１２１’として記憶される。

【００７４】最後にステップ３１０の処理によって、以上の結果得られた暗号化データ１２１’、差分データ１２２’、差分データ１２３’、・・・が暗号化画像データとしてフロッピーディスクに保存される。

【００７５】次に、図９を参照して、本第２実施形態に係る暗号化復号化装置１０を復号化装置として動作させた場合の暗号化復号化装置１０の作用について説明する。なお、図９は、オペレータによって復号化処理の指示が入力された際に記憶装置２２から読み出されて実行される復号化処理プログラムの概略フローチャートである。

【００７６】まずステップ３５０では、フロッピーディスクに記録されている復号化の対象とする暗号化画像データをフロッピーディスクドライブ２６によって入力して記憶装置２２に記憶する。

【００７７】次のステップ３５２では、上記第１ブロックの画像データに相当する暗号化データに対して復号化を行ない、この結果得られた画像データ、すなわち第１画像データを記憶装置２２に記憶する。ここでの復号化方法は暗号化方法に対応した方法とされる。

【００７８】次のステップ３５４では、上記ステップ３

５２によって記憶された第１画像データと、上記ステップ３５０によって入力及び記憶された暗号化画像データのうちの第１ブロック以外のブロックの画像データに対応する差分データの１つとの画素毎の和分を算出して記憶装置２２の対応する差分データの記憶領域に記憶（上書き）する。本ステップ３５４によって算出された値は、算出に用いた差分データに対応する画像データに相当する。

【００７９】次のステップ３５６では、第１ブロック以外の全てのブロックの差分データについて上記第１ブロックの画像データとの和分の算出及び記憶が終了したか否かを判定し、終了していない場合は上記ステップ３５４へ戻り、終了した時点でステップ３５８に移行する。

【００８０】次のステップ３５８では、上記ステップ３５２によって記憶装置２２に記憶された第１ブロックの画像データと上記ステップ３５４及び３５６の繰り返し処理によって記憶装置２２に記憶された第１ブロック以外のブロックの画像データとを合成して１つの画像データとした後、次のステップ３６０では、該１つの画像データをフロッピーディスクドライブ２６によってフロッピーディスクの空き領域に出力した後に、本復号化処理プログラムを終了する。

【００８１】図１０には、１枚の長尺状の画像に対応する画像データを図７に示した暗号化処理プログラムで暗号化することによって得られた暗号化画像データを図９に示した復号化処理プログラムの処理対象とした場合の復号化画像データ（原画像データ）生成の流れが示されている。

【００８２】同図に示すように、図９のステップ３５０の処理によってフロッピーディスクから入力された復号化対象とする暗号化画像データのうちの暗号化データ１２１’は、ステップ３５２の処理によって復号化されて第１ブロック１２１の画像データとして記憶される。

【００８３】その後、ステップ３５４及び3’５６の繰り返し処理によって、第１ブロック１２１の画像データと差分データ１２２’、１２３’、・・・との画素毎の和分が算出され、算出された和分が第２ブロック１２２の画像データ、第３ブロック１２３の画像データ、・・・として記憶される。

【００８４】最後にステップ３５８及び３６０の処理によって、以上の結果得られた第１ブロック１２１の画像データ、第２ブロック１２２の画像データ、第３ブロック１２３の画像データ、・・・が合成されて１枚の画像に対応する復号化画像データ（原画像データ）１２０としてフロッピーディスクに保存される。

【００８５】以上詳細に説明したように、本第２実施形態に係る暗号化復号化装置では、暗号化を行なう場合には、暗号化の対象とする画像の画像データの全ての領域を暗号化せずに、一部の領域の画像データのみを暗号化し、他の領域の画像データについては暗号化する領域の画像データとの差分のみを演算することによって全体的な暗号化画像データを生成しているので、画像データの全ての領域に対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができると共に、復号化を行なう場合には、暗号化画像データの全ての領域を復号化せずに、一部の領域の画像データに対応する暗号化データのみを復号化し、他の領域の画像データについては復号化した画像データとの和分のみを演算することによって全ての領域の復号化画像データを生成しているので、画像データの全ての領域に対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる。

【００８６】なお、本第２実施形態では、第１ブロック以外のブロックの画像データの差分を算出する際の対象を第１ブロックの画像データとした場合について説明したが、本発明はこれに限定されるものではなく、例えば、第１ブロック以外の第Ｎブロック（Ｎ＝２、３、・・・）の画像データの差分を算出する際の対象を第（Ｎ－１）ブロックの画像データとすることもできる。このように暗号化画像データを生成した場合、該暗号化画像データを復号する際には暗号化された第１ブロックの画像データを暗号化方法に対応した復号化方法によって復号した後に、この復号された第１ブロックの画像データに第２ブロックの画像データに対応する差分データを画素毎に加算することによって第２ブロックの画像データを復元し、この第２ブロックの画像データに対して第３ブロックの画像データに対応する差分データを画素毎に加算することによって第３ブロックの画像データを復元する、という手順を第１ブロック以外の全てのブロックの画像データについて繰り返すことによって全てのブロックの画像データを再現することができる。

【００８７】また、本第２実施形態では、実際に暗号化を行なう画像データを１ブロック分の画像データのみとした場合について説明したが、本発明はこれに限定されるものではなく、複数のブロックの画像データについて暗号化する形態としてもよい。

【００８８】また、本第２実施形態では、暗号化処理の途中段階で生成される暗号化データ１２１’、差分データ１２２’、・・・や復号化処理の途中段階で生成される第１ブロック１２１の画像データ、第２ブロック１２２の画像データ、・・・を記憶装置２２に記憶する場合について説明したが、本発明はこれに限定されるものではなく、フロッピーディスクに直接記録する形態としてもよい。

【００８９】また、本第２実施形態では、差分データを算出する場合の領域を当該ブロックの画像データの全ての領域とした場合について説明したが、本発明はこれに限定されるものではなく、当該ブロックの画像データの一部の領域とする形態としてもよい。従って、例えば、第１ブロック１２１の画像データ及び第２ブロック１２

２の画像データの各々のサイズが異なる場合でも差分データを算出することが可能である。

【００９０】また、本第２実施形態では、差分データの各々が、どのブロックの画像データとの差分であるのか、といった情報を暗号化画像データに保持しない場合について説明したが、本発明はこれに限定されるものではなく、この情報を保持する形態としてもよい。

【００９１】また、本第２実施形態では、暗号化処理プログラム及び復号化処理プログラムを記憶装置２２に記録しているが、本発明はこれに限定されるものではなく、該プログラムをフロッピーディスクに記憶すると共に、ワークステーション１２にハードディスクを備え、フロッピーディスクから該プログラムを読み取り、ハードディスクにインストールしてもよい。また、有線又は無線のネットワークに電話回線等の伝送手段により伝送してインストールしてもよい。なお、該プログラムをフロッピーディスクに記憶することに限定されず、ＣＤ－ＲＯＭ、磁気テープに該プログラムを格納し、該ＣＤ－ＲＯＭ、磁気テープからパソコンのハードディスクにインストールしてもよい。また、該プログラムを格納したハードディスクを備えるようにしてもよい。更に、パソコンのハードディスクやＲＡＭに直接プログラムを書き込むようにしてもよい。このように上記プログラムは、有形の記憶媒体及び伝送手段の少なくとも一方により流通することができる。

【００９２】また、本第２実施形態では、暗号化画像データをフロッピーディスクに記録する場合について説明したが、本発明はこれに限定されるものではなく、ハードディスク等の磁気ディスク、ＣＤ－Ｒ等の光ディスク、光磁気ディスク等に記録する形態としてもよい。この場合、上記ハードディスク、ＣＤ－Ｒ等の各メディアが本発明の請求項１０記載の記録媒体に相当することになる。

【００９３】

【発明の効果】以上説明したように請求項１及び請求項５記載の発明によれば、複数の画像データの全てを暗号化せずに、一部の画像データのみを暗号化し、残りの画像データについては暗号化する画像データと直接的又は間接的に画素毎の差分を演算することによって全ての暗号化画像データを生成しているので、全ての画像データに対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができる、という効果が得られる。

【００９４】また、請求項２及び請求項６記載の発明によれば、暗号化画像データの全てを復号化せずに、実際に暗号化された暗号化データのみを復号化し、残りの画像データについては復号化した画像データ又は復号化した画像データに基づく画像データとの加算を行なうことによって全ての復号化画像データを生成しているので、全ての画像データに対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる、という効果が得られる。

【００９５】また、請求項３及び請求項７記載の発明によれば、１画像を表す画像データの全ての領域を暗号化せずに、一部のブロックの画像データのみを暗号化し、残りのブロックの画像データについては暗号化するブロックの画像データと直接的又は間接的に画素毎の差分を演算することによって全体的な暗号化画像データを生成しているので、画像データの全ての領域に対して暗号化を行なう場合に比較して暗号化のための処理時間を大幅に短縮することができる、という効果が得られる。

【００９６】更に、請求項４及び請求項８記載の発明によれば、暗号化画像データの全ての領域を復号化せずに、一部の領域の画像データに対応する暗号化データのみを復号化し、残りの領域の画像データについては復号化した画像データ又は復号化した画像データに基づいて求めた画像データとの加算を行なうことによって全ての領域の復号化画像データを生成しているので、画像データの全ての領域に対して復号化を行なう場合に比較して復号化のための処理時間を大幅に短縮することができる、という効果が得られる。

【図面の簡単な説明】

【図１】実施の形態に係る暗号化復号化装置の外観図である。

【図２】実施の形態に係る暗号化復号化装置の概略構成を示すブロック図である。

【図３】第１実施形態に係る暗号化復号化装置の暗号化処理プログラムの流れを示すフローチャートである。

【図４】第１実施形態に係る暗号化復号化装置の暗号化画像データ生成の流れを示す概念図である。

【図５】第１実施形態に係る暗号化復号化装置の復号化処理プログラムの流れを示すフローチャートである。

【図６】第１実施形態に係る暗号化復号化装置の復号化画像データ（原画像データ）生成の流れを示す概念図である。

【図７】第２実施形態に係る暗号化復号化装置の暗号化処理プログラムの流れを示すフローチャートである。

【図８】第２実施形態に係る暗号化復号化装置の暗号化画像データ生成の流れを示す概念図である。

【図９】第２実施形態に係る暗号化復号化装置の復号化処理プログラムの流れを示すフローチャートである。

【図１０】第２実施形態に係る暗号化復号化装置の復号化画像データ（原画像データ）生成の流れを示す概念図である。

【符号の説明】

１０　暗号化復号化装置（暗号化装置、復号化装置）
１２　ワークステーション／パーソナルコンピュータ
１４　ＣＰＵ
１６　ＲＯＭ
１８　ＲＡＭ

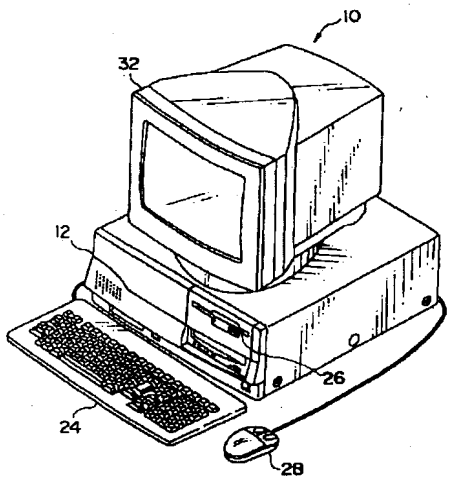
19

２０　入出力ポート
２２　記憶装置
２４　キーボード

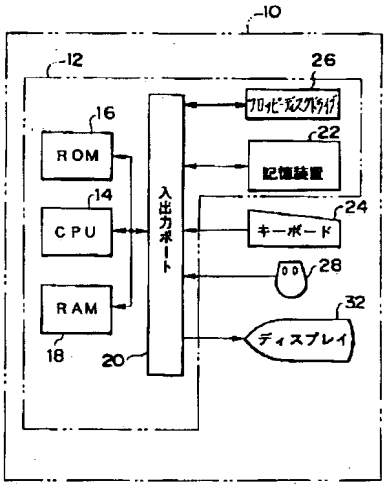
20

２６　フロッピーディスクドライブ
２８　マウス
３２　ディスプレイ

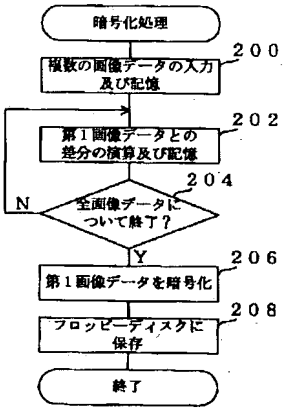
【図１】



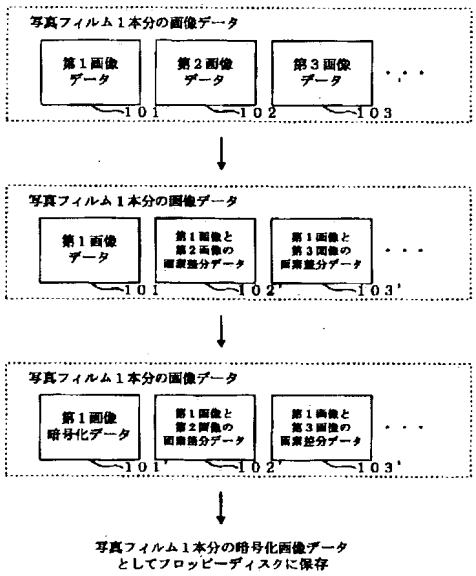
【図２】



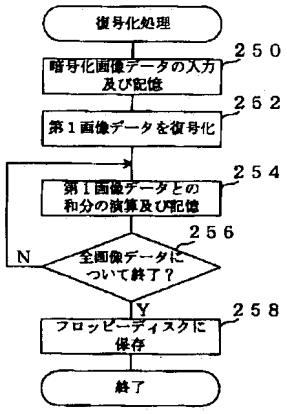
【図３】



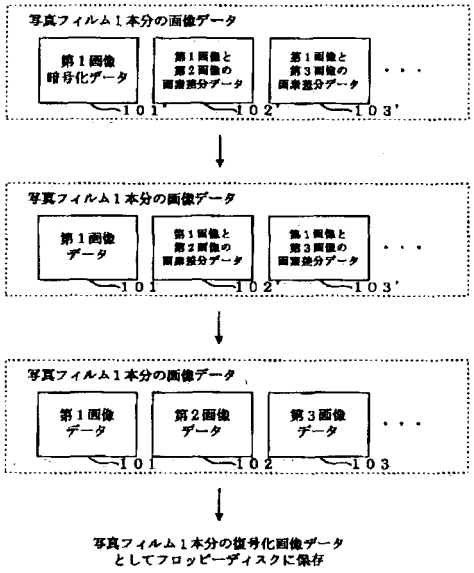
【図４】



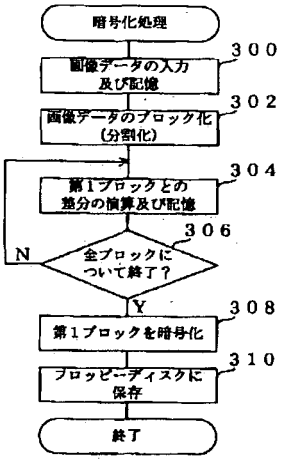
【図５】



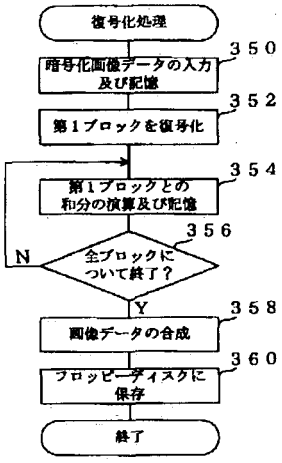
【図６】



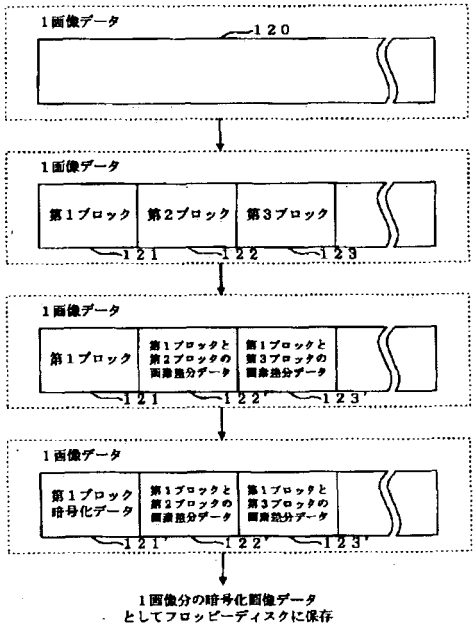
【図７】



【図９】



【図８】



【図１０】